ETHOS PRIVACY

SENTINEL LLC

PRIVACY METRICS

The Top Three Most Important Metrics for Monitoring Your Privacy Culture

It's easy to say that you're creating a privacy-aware culture in your organization, but it's much harder to know whether you've been successful in creating that culture. This often stems from the difficulty of monitoring your progress along the way and clearly defining what success looks like and how to measure it.

In order to have some confidence that the policies and processes you've put into place are working, you must have an actionable set of metrics that you monitor, report, and use to provide incentives for your employees and vendor population. But just because something can be counted does not mean the number conveys valuable information. It is vital that the metrics you use are tied to your organization's goals and lead to actionable steps to help you improve your privacy outcomes.

Working from publicly available data and the experience of seasoned privacy professionals, this white paper describes key metrics for baselining the effectiveness of your privacy program and helps you establish a baseline for monitoring them going forward. While each organization will have different priorities, obstacles, and unique situations dictated by their business model, organizational mission, or applicable jurisdiction, each of these metrics is designed to support a fundamental component of a privacy program, which should then generally applicable for most organizations.

By no means are the metrics described in this paper the only things that you should measure, but structuring your metrics program around these fundamentals will provide you direction in creating and monitoring other metrics that serve a similar purpose: To give you information to support decision making based on a realistic picture of what's actually happening within your organization.

An area as complex and ever-changing as privacy is no place to be navigating in the dark.

Chapter 1: What makes a good metric?

Part of a great metrics program is managing expectations. In addition to metrics being useful to manage day-to-day activities, they can also be used to influence others and drive accountability and change.

The number of things one can measure these days is, well, immeasurable. Creating a metrics program because you're told you need a metrics program will likely leave you swimming in a sea of numbers that don't provide direction. This situation is no help to your team or your organization. So, understanding the purpose your metrics program aims to serve is the first step toward developing your program. From that, you can determine what's worth measuring in order to obtain value from the program.

There are a number of different ways to organize and structure metrics, but in general they encapsulate the following concepts:

- **Activity: Measuring counts of things.** The number of things done by a person or system over a period of time. How many people did a person train in the last six months? How many records did a certain form on your web site collect last week?
- **Trend: Measuring things against another variable, typically time.** The number of things generated by actions taken by people or a system over a period of time. How many PIAs did those trained people conduct over the last six months?
- **Outcome: Measuring the extent to which you are achieving your goals.** The effect that the outputs or activities may have had on your business goals. How many fewer privacy complaints were escalated to your privacy team due to training more of your employees?

In all cases, you want to make sure your metrics are obtainable, repeatable, and outcome-focused. There's an old adage about metrics: If something is easy to measure, it's probably not valuable; and if it's valuable, it's probably not easy to measure. Maintaining metrics is often manual, taking scarce resources from other tasks. Even automated metrics usually require significant human intervention in order to draw valuable insights, so it's important that the insight you get from them exceeds the ongoing effort to capture and report them. Which means you need to use them! Understanding how you will use your metrics and communicate them to others is critical to obtaining value.

Metrics for leadership

The metrics you use when presenting to your CEO or board of directors will be very different from those you use to drive performance and expectations within your team. The CEO and board will want you to focus on output and impact — what has been done and how has it affected the organization's performance or current status.

Remember that when reporting metrics to executives, the numbers and the story around them are equally important. All that work you did to capture detailed metrics can easily be undone by an executive saying that they don't understand why you are telling them something, or what they should do about it. Don't just present raw numbers. Each visual or number should be as simple as possible, with a clear explanation of why it's being reported and what action should be taken in response.

Metrics for the privacy team
Measuring is management. The metrics you report to your privacy team or use in managing performance should be focused on activity and output — who is doing what and what is the output from these activities? Metrics can be used to both measure the effectiveness of activities (i.e., how well are they meeting anticipated goals?) as well as efficiency (i.e., how much output is being produced per unit input?). And don't forget to celebrate successes! Using metrics to demonstrate the privacy team's impact on the organization and how their work meets its overall goals, perhaps on a semi-annual basis, can give the team a real boost.

Metrics mistakes
The most common metrics mistakes companies make are over-measuring and under-utilizing the metrics they collect. There's no sense in measuring things that aren't valuable, and the same goes for not using the metrics you collect to shape organizational practices for future success. You should always be able to articulate the "why" of each metric, and you should be constantly checking and adjusting to make sure the data you're collecting continues to matter.

Another mistake is not evolving your metrics program over time. It may well be that a metric is vital to establishing a program, but once the program is up and running, you no longer need to be monitoring that data. For example, if you are establishing a training program, initially you will want to focus on getting to 100% (or close) of people in your desired group being trained. After that you're into maintenance mode and your metric can evolve into how many of those people have been trained in the previous 12 months.

Once that is running along without problem (or in parallel), you may want to confirm that people who have been trained actually act differently from those who don't. This is a lot harder than counting the number of people who turned up to a training class. While this is the one metric that really matters in achieving valuable training, you obviously can't start there.

As your program matures, you will find there is new data that better represents progress toward certain goals or the health of the program. It's important to build these periodic re-examinations into any metrics program to establish whether what was useful is still valuable or should be updated.

In the following chapters we will highlight important metrics that companies beginning to develop a metrics program should work toward.

Chapter 2: Data Subject Rights

Data Subject Rights (DSRs) is an area where organizations may have legal requirements depending on their jurisdiction. One common metric organizations capture is the number of data subject rights requests they receive — which is unsurprising, given it's a requirement of the CCPA. While the raw number and how it's trending are important to know, there are other important — and likely more valuable — metrics you should also be tracking. Remember, even one access request could create a problem if you take too long to respond to it.

Metric: Median time to respond to data subject rights requests, month-over-month
Goal: Consistently within legally mandated timeframe; trending down or remaining steady

Obviously, it's important that your response time to data subject rights requests is within the legally mandated time frame, but this metric is also an important key performance indicator (KPI) to ensure your systems are working smoothly. An increase in time between receipt of a DSR request and its resolution could indicate that systems are breaking down and you're not able to keep up with an increased volume of requests, or it could be a result of turnover and a need to retrain new people. It's important to understand root causes and not go with the first interpretation of what a metric may be telling you.

The CCPA regulations suggest you track DSR response time in median number of days, but you may have other ways to track for various reasons that align with your particular goals, risk levels, and audience.

CCPA

Some regulations require organizations to compile specific metrics. The California Consumer Privacy Act (CCPA) regulations, for example, have requirements around tracking data subject access requests, and the GDPR's language around accountability demands that you be able to produce records of processing. This is the bare minimum baseline, and your first task should be to identify base-level metrics requirements that you can build from.

Your legal obligations are based on some combination of four main factors: your industry, the kind of personal information you process, the jurisdictions in which you do business, and what you do with the personal information you collect. Understanding these key elements will help you determine what metrics you are legally required to compile.

However, just because a metric is legally required does not mean it's an important indicator of program health. A metric generated for compliance is different from a metric that is generated because you have decided it helps you understand how your program is performing.

For example, while the CCPA requires you compile a raw number of data subject access requests, producible upon request, you may decide that what's important to your privacy program is tracking the change in monthly data subject access requests over time. Those are two very different metrics, as we discuss in Chapter 2.

For some organizations, where customer service is of the highest priority and there's a robust privacy program in place, anything more than essentially instantaneous will be of note — they'll have an automated system in place that provides anyone with their data in an easily digestible format. So, their metric might track any requests that the automated system isn't able to handle, or the number of questions or complaints that are received after an individual receives their automated result.

For small organizations light on privacy budget and staffing, or where DSR requests are relatively rare due to the nature of their businesses and privacy isn't a key marketing point, anything under the legally mandated time frame will be fine. That's why the month-over-month trend is the key metric to follow.

Once you understand your goal and collect some metrics over time, you'll need to evaluate the data and trends you are receiving. For example, what's leading to an increase in time to respond? Is there an increase in volume of requests? If that correlates with an increase in revenue and sales, you might simply need to build out your team. But if that correlates with a new product launch, it might be that the product is leading to a loss in trust with your customers. Being able to understand the reason why a metric is changing is key to being able to make the right course corrections in response.

Chapter 3: Complaints & Inbound Communications

While there are very few legal requirements around how an organization manages privacy complaints and inquiries, these can be leading indicators to enforcement actions down the road. Much like DSR requests, it's important that you handle them quickly and to the satisfaction of the person/body making the inquiry. On top of gaining an understanding of the success of your response, for complaints and inquiries, you also want to understand who they are coming from. A complaint from a regulator or the media can mean a lot more trouble for your company than a complaint from a data subject. But, of course, an unresolved complaint from a data subject may mean their next stop is the regulator's office — so tracking those complaints is very important.

Metric: Number of complaints and from what category of complainant (data subjects, media, regulators)
Goal: Steady and trending down

It's unrealistic to think you'll get to a place where you consistently have no privacy complaints. You can't make everybody happy all the time, and some of those unhappy people are bound to complain. So, set an acceptable range for your organization. This number will depend on the amount and types of personal information you process, how much contact you have with data subjects in general, and your risk tolerance. Revisit that number regularly and adjust it according to changes in your business.

The number of complaints you receive has an important story to tell about your privacy program as a whole. In general, there are two reasons for privacy complaints: poor data privacy practices and unsuccessful communication with data subjects — meaning it helps gauge the internal systems and processes you've put in place, how well your staff is trained on privacy concerns, and how well your external-facing communications are explaining your data practices. Pay attention to how many complaints you receive; when you see a dramatic change look for trends in what the complaints are about and trace it back to the source.

It's important to note that certain events may cause a temporary uptick in the number of complaints you receive. For example, sending a notification that you changed your privacy notice, or releasing a new feature set that involves personal information is likely to trigger complaints. When determining whether this metric is cause for concern, these events must be considered.

Learn More

Ethos Privacy is committed to the successful implementation of a privacy program that will strengthen your company's brand, reputation, and overall trust in your organization. We offer both strategic consulting and a software platform to help define, measure, and optimize the right privacy program for your unique organization.

Contact info@sentinelcsg.com to find out more about scheduling a metrics workshop customized for your organization.